UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with the online storage accounts stored at premises controlled by Apple, Inc., as described in Attachment A	)	Case No. 3:23-mc-477

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2)	Distribution of Child Pornography

The application is based on these facts:

See Affidavit of Justin Moshofsky attached to Search Warrant Application.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Justin Moshofsky, Special Agent, HSI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone at 4:22 pm *(specify reliable electronic means)*.

Date: June 7, 2023

Youlee Yim You
Judge's signature

City and state: Porland, Oregon

Hon. Youlee Yim You, United States Magistrate Judge
Printed name and title

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with AppleID **jaredtbates1995@gmail.com**, Directory Services Identifier **11787337509**, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B

Particular Things to Be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber

Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. All activity, connection, and transactional logs for the App Store (including purchases, downloads, and updates of Apple and third-party apps).

Apple is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes evidence and/or instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) (Distribution of Child Pornography), from September 1, 2020, to December 31, 2020, including, for the account listed in Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the Apple Media Services account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the distribution of child pornography and the account subscriber, including the application download history for the Tumblr application; and

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information).

III. Search Procedure

a. The warrant will be executed under the Electronic Communications Privacy Act, 18 U.S.C. § 2703(a), (b)(1)(A), and (c)(1)(A), and will require Provider to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of this attachment.

b. During its review of the information received from Provider under this warrant, law enforcement will segregate the information into two groups: (i) information that is responsive to the warrant and that the government may therefore seize; and (ii) information that is not responsive to the warrant. This review will be performed within a reasonable amount of time not to exceed 180 days from the date the warrant is executed. If the government needs additional time to conduct this review, it may seek an extension of time from the Court.

c. Information that is responsive to the warrant will be copied onto a separate storage device or medium. Responsive information may be used by law enforcement in the same manner as any other seized evidence. Information that is not responsive to the warrant will be sealed and stored on a secure medium or in a secure location. Nonresponsive information will not be reviewed again without further order of the Court (e.g., subsequent search warrant or order to unseal by the district court).

d. The government will retain a complete copy of the information received from Provider for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing

potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

DISTRICT OF OREGON, ss: AFFIDAVIT OF JUSTIN MOSHOFSKY

Affidavit in Support of an Application for a Search Warrant for an Apple Account

I, Justin Moshofsky, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the U.S. Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI") and have been since September 2019. I am currently assigned to the child exploitation unit in the HSI office in Portland, Oregon. Previously, I was assigned to the HSI office in Portland as a Criminal Analyst while employed by the Oregon Air National Guard. In that capacity, I supported criminal investigations and prepared materials for prosecution. My formal law enforcement training includes successfully completing the 23-week HSI basic training course at the Federal Law Enforcement Training Center in Glynco, Georgia. During that training I learned how to conduct child exploitation investigations. Since then, I have also assisted federal and state partners on many child exploitation investigations. As a result, I have become familiar with the ways that child pornography is shared, distributed, and/or produced, including the use of various social media websites (Facebook, Twitter, Kik, Snap Chat, Discord, etc.), "cloud" based storage, and peer-to-peer (P2P) networks. I know individuals involved in child exploitation will "collect" or store images and/or videos on various media devices they routinely keep at their residences, or store in offsite locations such as "cloud" based storage. I have also become familiar with jargon or slang terms that people involved in child exploitation will use to discuss their activities. Additionally, I have become familiar with how child pornography is sold,

traded, and distributed on the "dark net," often being purchased with digital currency such as Bitcoin, Ripple, and others.

2. I submit this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple Inc. ("Apple" or "Provider") to provide information associated with the following account:

- Jaredtbates1995@gmail.com, Directory Services Identifier ("DSID") 11787337509 (the "Account")

The Account is further described in Attachment A to my affidavit. As set forth below, I have probable cause to believe that the Account contains evidence, as set forth in Attachment B to my affidavit, of violations of 18 U.S.C. § 2252A(a)(2) (Distribution of Child Pornography) (the "Target Offense").

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Target Offense

4. 18 U.S.C. § 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography using any means or facility of interstate or foreign commerce, or that has been

mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

Relevant Electronic and Wire Communication Statutes

5. The relevant federal statutes involved in the disclosure of customer communication records for the requested data in the Account are as follows:

a. 18 U.S.C. § 2703(a) provides, in part that a governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court of competent jurisdiction."

b. 18 U.S.C. § 2703(b)(1) provides, in part that a governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication without the required notice to the subscriber or customer, if the governmental entity obtains a warrant issued by a court of competent jurisdiction."

c. 18 U.S.C. § 2703(c)(1) provides, in part that a governmental entity may require a provider of electronic communication service or remote computing service to disclose non-content subscriber information if the governmental entity obtains a warrant issued by a court of competent jurisdiction, although that is not the only way in which the government may obtain non-content subscriber information.

d. 18 U.S.C. § 2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole

or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," with certain exceptions not applicable here.

e. 18 U.S.C. § 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication."

f. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2703(a), (b)(1)(A), (c)(1)(A), and 2711. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Summary of Probable Cause

6. In March 2021, HSI received CyberTipline Reports indicating that multiple Tumblr accounts uploaded child exploitative material between about September 22, 2020, and December 8, 2020. After connecting the CyberTipline Reports to the residence of Jared T. Bates ("BATES"), HSI executed a search warrant at BATES' residence. During the search warrant execution, BATES admitted in a *Mirandized* interview to distributing child pornography using the Tumblr application on his Apple iPhone. BATES also said that he would repeatedly delete and re-download the Tumblr application from his Apple iPhone as part of his process of distributing child pornography. Accordingly, this search warrant application seeks BATES' Tumblr application download history from Apple to determine whether BATES had the Tumblr application on his Apple iPhone on the dates the CyberTipline Reports indicate child pornography was distributed.

Statement of Probable Cause

I. Background on Investigation

7. In March 2021, the Oregon Internet Crimes Against Children ("ICAC") Task Force sent HSI Portland 17 CyberTipline Reports from the National Center for Missing & Exploited Children ("NCMEC") indicating that multiple Tumblr accounts uploaded images and videos of child exploitative material ("CEM") between about September 22, 2020, and December 8, 2020. Fourteen of the 17 CyberTipline Reports were linked to Internet Protocol ("IP") address 24.20.61.61 and records received from Comcast stated that BATES was the internet subscriber for that IP address. Additionally, the email address, "jaredtbates1995@gmail.com," which matched the name and birth year of BATES, was used to register the Tumblr accounts associated with three of the CyberTipline Reports. More detail about the CyberTipline Reports and initial investigation into them is set forth in Exhibit 1 to this affidavit, which is incorporated by reference and is a prior affidavit I swore out in case number 3:21-mc-975.

8. On September 3, 2021, the Honorable Stacie F. Beckerman, United States Magistrate Judge, issued a search warrant for BATES' residence in case number 3:21-mc-975. *See* Ex. 1. HSI agents executed that search warrant on September 7, 2021. BATES was not present during the search. Investigators located BATES at his job in possession of his Apple iPhone 11, with serial number C7CZN0BDN731 (the "Apple iPhone 11"). BATES' Apple iPhone 11 was seized under the search warrant and investigators interviewed BATES. After waiving his *Miranda* rights, BATES admitted to repeatedly distributing CEM from his Apple iPhone 11 using the Tumblr application. BATES explained that when Tumblr would close his

account for distributing CEM, BATES would delete the Tumblr application and any downloaded CEM from his cell phone. Later, BATES would re-download the Tumblr application, create a new Tumblr account, and distribute child pornography on Tumblr until the account was disabled.

9. In September 2021, under the search warrant, investigators forensically examined several seized digital devices, including BATES' Apple iPhone 11. During the examination, I saw that BATES' iCloud account on his Apple iPhone 11 was registered to the email address "jaredtbates1995@gmail.com," the same email address associated with three of the CyberTipline Reports mentioned above. I also saw multiple video and image files which met the definition of child pornography. For example, BATES' Apple iPhone 11 contained the following video:

- File Name: trim.0233D2E0-9516-4418-831F-37A48072820A.MOV
- MD5: 3D5469F5092D07016BFAB249DD8461E9
- Duration: 44 seconds
- Description: A video that depicted an infant girl, who appears to be less than 1 year of age, laying on a blanket naked. The infant is approached by an adult male who placed his penis in the infant's mouth while the infant attempted to block the act. The adult said, "she doesn't even cry, see."

II. Investigation into BATES' Tumblr Download History

10. With this search warrant, I seek to obtain BATES' Tumblr application download history for the period from September 22, 2020, to December 8, 2020, the dates the CyberTipline Reports indicate child exploitative materials were distributed. Although this information dates to 2020, I believe that it may still be in Apple's possession based on information received from Apple. Specifically, on April 29, 2023, I received notice from Apple that "Apple Media

Services" retains records from user downloads within the App Store. Apple stated that third-party application downloads, such as Tumblr, would be logged according to the Apple ID to individual Apple Accounts.

11. This information is also relevant to confirming that BATES was the person who distributed the CEM reported in the CyberTipline Reports. In this case, BATES said that his Apple iPhone 11 was used to create Tumblr accounts to distribute CEM to other Tumblr users. BATES also said that his distribution of CEM through Tumblr followed a pattern of downloading, deleting, and re-downloading the Tumblr application so that he could continue distributing CEM after Tumblr disabled his accounts. So, information related to whether the Tumblr application was downloaded and remained on BATES' Apple iPhone 11 during the dates the CEM reported in the CyberTipline Reports was distributed, is relevant to determining whether BATES was, in fact, the person who distributed that CEM. BATES' statements are also consistent with my training and experience and from what I know from speaking to other law enforcement officers. Specifically, I know that some individuals who are interested in child pornography attempt to hide their interest in child pornography from roommates, family, and employers and, therefore, engage in cyclical patterns where applications are installed, criminal activity is conducted, and evidence is later removed from the device—like BATES admitted to in his *Mirandized* interview.

12. Additionally, I know from my review of the data extracted from BATES' Apple iPhone 11 that BATES' personal email account (jaredtbates1995@gmail.com) was registered to BATES' iCloud and that the Apple iPhone 11 contained numerous CEM images and videos, some of which visually matched the CEM reported in the CyberTipline Reports. Thus, based on

the statements made by BATES during his *Mirandized* interview, my training and experience, and information seen through a review of his device, I believe that Apple has records relating to the repeated download of the Tumblr application on BATES' Apple iPhone 11, including for the dates of the CyberTipline Reports, or from September 22, 2020 to December 8, 2020.

Records Held by Provider

13. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

14. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. App Store and the iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through the iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through the iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS. Apple provides these services through "Apple Media Services."

b. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

c. iMessage and FaceTime allow users of Apple devices to communicate in real time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

d. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices. iCloud Backup allows users to create a backup of their device data, meaning that backups of

entire devices (such as iPhones, iPads) for particular points in time can be stored in an iCloud account.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

15. Apple services are accessed through an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

16. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including

the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

17. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

18. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may

maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

19. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups (such as backups of iPhones, iPads, and other devices from particular points in time), which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on

iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

20. In my training and experience, evidence of who was using an Apple iPhone and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. BATES' use of "Apple Media Services" to download Tumblr will be confirmed by records maintained by Apple. BATES' use of Tumblr to distribute child pornography will be corroborated by the specific application download records provided by Apple.

21. For example, the download history provided by Apple associated with BATES' Apple ID may provide corroboration of the confession given by BATES concerning the offense under investigation and help align the creation of 14 separate Tumblr accounts as reported in multiple CyberTipline Reports. Based on my training and experience, social media accounts created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation, are commonly logged and the evidence is maintained by the service provider.

22. In addition, the Apple iPhone user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing,

such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Records provided by Apple may confirm BATES' ownership of the Apple iPhone 11, operation of the Apple iPhone 11 to distribute child pornography as admitted by BATES, and the confirmation of BATES downloading Tumblr to his phone at least 14 times prior to his distribution of child pornography.

23. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

24. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user.

Nature of Examination

25. During its review of the information received from Provider under this warrant, law enforcement will segregate the information into two groups: (i) information that is

responsive to the warrant and that the government may therefore seize; and (ii) information that is not responsive to the warrant. This review will be performed within a reasonable amount of time not to exceed 180 days from the date the warrant is executed. If the government needs additional time to conduct this review, it may seek an extension from the Court.

26. Information that is responsive to the warrant will be copied onto a separate storage device or medium. Responsive information may be used by law enforcement in the same manner as any other seized evidence. Information that is not responsive to the warrant will be sealed and stored on a secure medium or in a secure location. Nonresponsive information will not be reviewed again without further order of the Court (e.g., subsequent search warrant or order to unseal by the district court).

27. The government will retain a complete copy of the information received from Provider for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Conclusion

28. I have probable cause to believe that BATES committed the Target Offense, and that evidence of that offense, as more fully described in Attachment B, are presently contained in the Account, which is more fully described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the Account described in Attachment A for the items listed in Attachment B and the examination and seizure of any such items found.

29. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney ("AUSA") Robert Trisotto. AUSA Trisotto informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

/s/ by Telephone
Justin Moshofsky
Special Agent
Homeland Security Investigations

Sworn in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone at 4:22 pm on June 7, 2023.

Youlee Yim You
HONORABLE YOULEE YIM YOU
United States Magistrate Judge

EXHIBIT 1

to the

Affidavit of HSI SA Justin Moshofsky

DISTRICT OF OREGON, ss: AFFIDAVIT OF JUSTIN MOSHOFSKY

Affidavit in Support of an Application for Search Warrants

I, Justin Moshofsky, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I have been employed as a Special Agent (SA) by Department of Homeland Security (DHS), Immigration and Customs Enforcement, Homeland Security Investigations (HSI) since September 2019. I am currently assigned to the child exploitation unit in the HSI office in Portland, Oregon. Previously, I was assigned to the HSI office in Portland as a Counterdrug Support Program Criminal Analyst while employed by the Oregon Air National Guard; my role was supporting criminal investigations and preparing materials for prosecution. My formal law enforcement training includes successfully completing the 23-week HSI basic training course at the Federal Law Enforcement Training Center in Glynco, Georgia. During that training I learned how to conduct child exploitation investigations. Since then, I have also assisted federal and state partners on ten separate child exploitation investigations and also have been partnered with senior SA's Clinton Lindsly & Josh Findley who are the primary investigators for our judicial district due to their exceptional field experience; these agents have over 20 years, collectively, in the field of child exploitation investigations. As such, I have become familiar with ways that child pornography is shared, distributed, and/or produced, including the use of various social media websites (Facebook, Twitter, Kik, Snap Chat, Discord, etc.), "cloud" based storage, and peer-to-peer (P2P) networks. I know individuals involved in child exploitation will "collect" or store images and/or videos on various media devices they routinely keep at their residences, or store in offsite locations such as "cloud" based storage. I have also become familiar with jargon or slang terms that people involved in child exploitation

will use to discuss their activities. Additionally, I have become familiar with how child pornography is sold, traded, and distributed on the "dark net," often being purchased with digital currency such as Bitcoin, Ripple, and others.

2. I have worked with agents involved in numerous investigations related to the sexual exploitation of children or the distribution, receipt, and possession of child pornography. I have participated in searches of premises and assisted in gathering evidence pursuant to search warrants, including search warrants in multiple child pornography investigations. I have participated in interviews of persons identified as possessing and distributing child pornography.

3. I submit this affidavit in support of an application for a search warrant authorizing searches of the person of **Jared BATES**, **BATES' Cell Phone**, **Subject Premises** located at 21961 NE Chinook Way #229, Fairview, Oregon 97024, and the Gmail account jaredbates1995@gmail.com (**Subject Email Account**), as described in Attachment A-1 and A-2 hereto, for contraband and evidence, fruits, and instrumentalities of violations of *18 U.S.C. § 2252A(a)(2)* – Distribution of Child Pornography and *18 U.S.C. § 2252A(a)(5)(B)* – Possession of or Accessing with Intent to View Child Pornography, collectively referred to as the "**Target Offenses**," as described in Attachments B-1 and B-2 hereto, including any digital devices or electronic storage media.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, a review of records related to this investigation, communications with others who have

/ / /

knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

5. *Title 18, United States Code, Section 2252A(a)(2)* makes it a crime to knowingly receive or distribute any visual depiction of a minor engaging in sexually explicit conduct that has been mailed or transported in interstate or foreign commerce or from knowingly reproducing any such visual depiction for distribution in interstate or foreign commerce or through the mails.

6. *Title 18, United States Code, Section 2252A(a)(5)(B)* makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term "child pornography" is defined in 18 U.S.C. § 2256(8), which is incorporated herein.

Background on Computers and Child Pornography

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I am aware that computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

8. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

9. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and

distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the internet, a worldwide network of interconnected computers and other devices, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously in the last several years. These drives can store thousands of high-resolution images. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on someone's person or inside his or her vehicle.

11. The internet affords collectors of child pornography multiple venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat (IRC), instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs such as LimeWire and eMule, and networks such as eDonkey, Gnutella, ARES, Tumblr, and BitTorrent, among others. Collectors and distributors of child pornography sometimes also use online resources such as "cloud" storage services to store and retrieve child pornography such as Mega or Dropbox. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an

/ / /

online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

12. An Internet Protocol (IP) address is a unique number that devices such as computers, routers, internet fax machines, printers, tablets, and sometimes phones, etc. use in order to identify and communicate with each other over a network. Each device must have its own unique IP address. An IP address can be thought of as a street address. Just as a street address identifies a particular building, an IP address identifies a particular Internet or network access device. When a user logs on to his/her Internet Service Provider (ISP), the user is assigned an IP address for the purpose of communication over the network. ISPs keep records of who IP addresses are assigned to by date and time, and can provide the internet access account associated with a designated IP address at a particular date and time. Similarly, cell phone service providers also generally keep IP records that can identify what device (cell phone) utilized the IP address at a certain date and time.

13. However, a person can conceal or mask their IP address by using a Virtual Private Network (VPN). A VPN gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your IP address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot. The encryption and anonymity that a VPN provides helps protect your online activities: sending emails, shopping online, or paying bills. VPNs also help keep your web browsing anonymous. VPNs essentially create a data tunnel between your local network and an exit node in another location, which could be thousands of miles away, making it seem as if you're in another place. VPN's can assist in hiding a user's browsing history, their IP address and location, location data for streaming, and a

user's web activity among other things. There are many VPN service providers that can be purchased for monthly fees or free versions. Depending on what VPN service is being used, the user can connect multiple devices at the same time. Based on my training and experience, many investigations involving the exploitation of children involve the use of VPNs in an attempt to avoid detention by law enforcement.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

15. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence or vehicle, and on computers and digital storage

media under their direct control. Such persons often maintain their collections, considered as prized possessions for long periods of time, and prefer not to be without their collections for any prolonged span of time. It is extremely common that they maintain their collection for years. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely. I know that images are still able to be found on computers and other storage media even when deleted; file directory pointers may be lost or destroyed but the files are often left for future overwriting and can be recovered by computer forensics techniques.

16. I also know from my training and experience that persons who download child pornography from the internet, and those who collect child pornography, frequently save images and videos of child pornography on their computers and/or transfer copies to other computers and storage media, including external hard drives, thumb drives, flash drives, SD cards, and CDs or DVDs. Moreover, it is common in child pornography investigations to find child pornography on multiple devices and/or storage media located in suspects' homes, rather than on a single device.

17. I know based on my training and experience that many social media applications can be directly accessed and used with one's cellular phone. Oftentimes, these applications require the user to download the "application" directly to their phone, which then allows seamless use between the cellular phone and the social media website.

Information Regarding NCMEC

18. The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit organization to serve as a

national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further their mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Programs. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Programs available to law enforcement and uses this information to help identify trends and create child safety and prevention messages. As a national clearinghouse, NCMEC also works with electronic service providers (ESPs), law enforcement, and the public in a combined effort to reduce online child sexual exploitation. NCMEC does not act in the capacity of or under the direction or control of any government or any law enforcement agency. NCMEC does not independently investigate and cannot verify the accuracy of the information submitted by reporting parties.

19. CyberTipline Reports are initially submitted to NCMEC. Anyone can submit a CyberTipline Report, although the majority of CyberTipline Reports I review are submitted by ESPs such as Google, Facebook, Instagram, Yahoo, Microsoft, Dropbox, and the like. CyberTipline Reports from ESPs typically contain information about the subscriber, such as the subscriber's username, email address, telephone numbers, and IP address history. CyberTipline Reports will also contain the child exploitation material that caused the ESP to initiate the report. That child exploitation material is often image or video files of child pornography as defined by federal law.

Information on Tumblr

20. Through my training and experience, as well as conversations with other experienced law enforcement officers and a review of materials available on the public website

for Tumblr, I have learned that Tumblr provides an online internet-based platform for people to post short-form blogs as well as posting photographic/video content; the goal of Tumblr is allow users to express themselves freely. Users can restrict access to the content they upload and/or manage private groups for sharing comments, photographic/video content, or links to other websites or photographic/video content. Many private groups need a specific invite in order to join. Tumblr provides users with unrestricted access to voice their opinion and share interests with people across the globe with a few caveats.

21. A subscriber, upon signing up for a Tumblr account, agrees not to use Tumblr to post or solicit content that features the abuse of a minor which includes suggestive or sexual content involving a minor or anyone that appears to be a minor, or that facilitates or promotes child sexual abuse. Tumblr further clarifies in its online policy that child harming content may include photos of real individuals, illustrations, animation, or text; the platform also warns users that posting or reblogging child sexual abuse material is a serious crime for which they have no tolerance. Tumblr warns the user explicitly that they will report all instances of child harming content to child protection organizations and law enforcement around the world, including NCMEC.

22. Online social media platforms such as Tumblr typically retain certain transactional information about the creation and use of each account on their systems. This information can include an email address used by Tumblr to correspond with the account user, a user-determined unique account name, the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, online

social media platforms often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

23. Collectors and distributors of child pornography often use online resources to store, retrieve, and share child pornography. Non-pornographic, seemingly innocuous images of minors are often found in online storage accounts that also contain child pornography. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

Statement of Probable Cause

Investigators Receive CyberTipline Reports Regarding Multiple Tumblr Accounts

24. In March 2021, HSI Special Agent (SA) Clint Lindsly was assigned to investigate information received by the Oregon Internet Crimes Against Children (ICAC) Task Force from National Center for Missing & Exploited Children (NCMEC); I was later assigned to assist the investigation. This information included 17 CyberTipline Reports involving several Internet Protocol (IP) addresses uploading numerous images and videos of child exploitative material to multiple corresponding accounts on Tumblr; of note, 14 accounts were reported to NCMEC by Tumblr. Of the 17 CyberTipline Reports, two were generated from other Tumblr users who identified posts containing Child Exploitative Material (CEM). Some of the information received from two CyberTipline Reports were duplicative of the information provided by the other CyberTipline Reports supplied by Tumblr. There is an additional report which supplements the original CyberTipline Report with additional posts, from one of the 14 accounts

associated with 24.20.61.61 (**Target IP Address**), that Tumblr identified as potential CEM. All 14 Tumblr-identified and reported user accounts were associated with **Target IP address**. Additionally, multiple accounts associated with **BATES** connected from various IP addresses consistent with the use of a VPN and various IP addresses consistent with the use of a cell phone serviced by Verizon Wireless. All 14 of the suspect Tumblr accounts were accessed from the **Target IP Address**, consistent with all of the accounts being controlled by the same user. In addition to consistent access from **Target IP Address**, shortly after Tumblr would shut down one account for CEM, another account would be created from **Target IP Address**. Of the 17 CyberTipline Reports associated with the distribution of child pornography, three of the accounts utilized an email address in the namesake of "Jared Bates" and his birth year of 1995 i.e., jaredtbates1995@gmail.com (**Subject Email Address**). Additionally, this same email address was used by **BATES** in his rental application for the **Subject Premises**. Based on these facts and others discussed in more detail below, I believe the user of these 14 Tumblr accounts was in fact **BATES**, who now resides at the **Subject Premises**.

25. As further discussed below, in March 2021, **BATES** moved from his former residence where the **Target IP Address** was previously assigned. **BATES** has obtained new internet service through Comcast, which is subscribed to **BATES** at the **Subject Premises**. Tumblr identifies and reports child sexual abuse imagery to NCMEC in their normal course of business. Specifically, I learned the following:

CyberTipline Report 80287864

26. On September 22, 2020, Tumblr reported three images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "jesusdidntsavemeforthis" with an email address of jaredtbates1995@gmail.com (**Subject Email**

Address). I downloaded and reviewed these images, of which at least one met the federal definition of child pornography. A description of the image follows:

> File Name: 630011090334629888_0_inline_image.jpg[1]
> MD5: 772730596c5d575107ebdb5442669d6f
> The image depicts a female child naked on a backlit platform. The female child was approximately 6 – 10 years of age. The female child was posed with her body contorted to hold her knees against her shoulders, waist raised. Legs were spread exposing her vagina.

CyberTipline Report 81100977

27. On October 8, 2020, following Tumblr shutting down the above account, Tumblr reported six images containing suspected child pornography which were uploaded by a new account created at **Target IP Address**, identified as "swimmingjudgeturtleroad" with an email address of jaredtbates1995@gmail.com (**Subject Email Address**). I downloaded and reviewed these images, of which all six images met the federal definition of child pornography. For example:

> File Name: 631458889790013440_0_inline_image.jpg
> MD5: fd8ba844a1fbd00f0871afb3274ae1e8
> The image depicts a female child standing naked in a bathroom. The female child was approximately 3 – 7 years of age. The female child was holding an erect adult penis in her hand and had her tongue out.

CyberTipline Report 81262604

28. Between October 10-11, 2020, following Tumblr shutting down the above account, Tumblr reported 22 images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "innerfestivalsportsshepherd" with an email address of jaredtbates1995@gmail.com (**Subject Email Address**). I downloaded and

[1] I believe that the file naming convention in each of the CyberTipline Reports described in this affidavit was created by Tumblr and may not be the actual file name of the uploaded image.

reviewed these images, of which at least seven met the federal definition of child pornography. For example:

> File Name: 631649954980642817_0_inline_image.jpg
> MD5: 8c8036a510dd386dd98843487bc9e63a
> The image depicts a female child laying on her back with her hands above her head, tied by rope. The female child was approximately 6 – 10 years of age. The female child had an adult male straddling her with his erect penis in her mouth.

CyberTipline Report 81602360

29. Between October 17-18, 2020, following Tumblr shutting down the above account, Tumblr reported four images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "automaticmoneyfriendapricot" with an email address of jonnyboyles@yahoo.com. I downloaded and reviewed these images, of which all four met the federal definition of child pornography. For example:

> File Name: 632286063278374912_0_inline_image.jpg
> MD5: 912f87fb051ee78098134f8f01ce82f3
> The image depicts two female children who were mostly naked. The female children were approximately 6 – 10 years of age. The second female child was performing oral sex on the first female child.

CyberTipline Report 81006419

30. Between October 18-19, 2020, following Tumblr shutting down the above account, Tumblr reported four images and four videos containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "qualitywombateggthing" with an email address of jonnyboyles@yahoo.com. I downloaded and reviewed these images and videos, of which all eight images and/or videos met the federal definition of child pornography. For example:

> File Name: 632377560790122496_0_inline_image.gifv
> MD5: a2edf5789b70362a4b91c164b99193e1

> The video depicts a female child laying naked on a bed. The female child was approximately 8 – 12 years of age. The female child licks the adult penis several times and then places the penis in her mouth.

CyberTipline Report 81948441

31. On October 24, 2020, following Tumblr shutting down the above account, Tumblr reported five images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "unlikelydeanroadeggs" with an email address of malcommarkstrom@yahoo.com. I downloaded and reviewed these images, of which at least two images met the federal definition of child pornography. For example:

> File Name: 632905518794604544_0_inline_image.jpg
> MD5: f44af95b5177ef9ad69a3476d20e0c9e
> The image depicts a female child laying on her back wearing only unzipped, ripped jean shorts. The female child was approximately 4 – 8 years of age. The female child was sucking on her thumb and the shorts were positioned so that her vagina was specifically exposed.

CyberTipline Report 81961358

32. On October 24, 2020, following Tumblr shutting down the above account, Tumblr reported five images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "sparklymoneyathletepanda" with an email address of malcommarkstrom@yahoo.com. I downloaded and reviewed these images, of which at least three images met the federal definition of child pornography. For example:

> File Name: 632929380167024641_0_inline_image.jpg
> MD5: ed59bf64ece9c13f2768d4c0b3886f88
> The image depicts a female child and male teen who were both naked. The female child was approximately 6 – 10 years of age; the male teen was approximately 14 – 18 years of age. The female child had both hands on the teen's erect penis, which was placed against her vagina.

/ / /

/ / /

/ / /

CyberTipline Report 82499408

33. On October 31, 2020, following Tumblr shutting down the above account, Tumblr reported six images and two videos containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "fantasticathletemuffinpasta" with an email address of malcommarkstrom@yahoo.com. I downloaded and reviewed this image and these videos, of which at least one image and two videos met the federal definition of child pornography. For example:

> File Name: 633567269138694144_0_inline_image.gifv
> MD5: 01fe1fba779b5e0f144219e44a2ccb38
> The video depicts a female child laying naked on her back. The female child was approximately 4 – 6 years of age. The female child was rubbing what appeared to be a toothbrush against the top of her vagina while an adult male used his finger to penetrate her vagina.

CyberTipline Report 82675833

34. Between November 6-8, 2020, following Tumblr shutting down the above account, Tumblr reported seven images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "partyboy20" with an email address of totov96409@diide.com. I downloaded and reviewed these images, of which at least four images met the federal definition of child pornography. For example:

> File Name: 634098110008786944_0_inline_image.jpg
> MD5: c73430be5475991a6a43461a5f8907bb
> The image depicts a female child wearing only socks. The female child was approximately 8 – 12 years of age. The female child was holding an erect adult penis in one hand and had her mouth around the penis while crossing her eyes.

CyberTipline Report 82675741

35. Between November 8-9, 2020, following Tumblr shutting down the above account, Tumblr reported 23 images and four videos containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as

"humongousfestivalskeletonzonk" with an email address of gexiv65905@jqjlb.com. I downloaded and reviewed these images and videos, of which at least 17 images and three videos met the federal definition of child pornography. For example:

> File Name: 634272828576956416_0_npf_video.mp4
> MD5: d1dff87be14d2f28b0bfc67550831f12
> The video depicts a female child who appeared to be naked. The female child was approximately 10 – 14 years of age. The female child was performing oral sex on an adult male.

CyberTipline Report 84314253

36. Between November 8-9, 2020, following Tumblr shutting down the above account, Tumblr reported 21 images and three videos containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "humongousfestivalskeletonzonk" with an email address of gexiv65905@jqjlb.com. I downloaded and reviewed these images and videos, of which at least 16 images and two videos met the federal definition of child pornography. For example:

> File Name: 634269235377487872_0_inline_image.gifv
> MD5: 31c85d0cd5802861b0aefd2fd63b713f
> The video depicts a female child sitting, naked between the legs of a naked adult male. The female child was approximately 4 – 6 years of age. The female child grabbed the erect adult penis with her hand and placed it in her mouth.

CyberTipline Report 82780966

37. Between November 12-13, 2020, following Tumblr shutting down the above account, Tumblr reported six images and three videos containing suspected child pornography uploaded by the account created at **Target IP Address**, identified as "malcyboysbackformore" with an email address of nadoy43272@testbnk.com. I downloaded and reviewed these videos, of which at least three videos met the federal definition of child pornography. For example:

> File Name: 634641210110279680_0_inline_image.gifv
> MD5: 77dddc63a73dcef6aedb3b293c74308a

> The video depicts one male child and three female children all of whom were naked. The children were approximately 4 – 8 years of age. One female child was performing oral sex for the male child; a second female was laying on her back, legs spread for a third female child who was rubbing the vagina of the second female child.

CyberTipline Report 82874529

38. Between November 13-15, 2020, following Tumblr shutting down the above account, Tumblr reported seven images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "illalwayscomeback" with an email address of wixose2120@testbnk.com. I downloaded and reviewed these images, of which two images met the federal definition of child pornography. For example:

> File Name: 634780931783376896_0_inline_image.png
> MD5: 294af7d55de204ac8b83419191252829
> The black and white image depicts a female child laying naked on a bed next to a naked adult male. The female child was approximately 8 – 12 years of age. The female child had her hand wrapped around the erect adult penis.

CyberTipline Report 83072099

39. Between November 22-23, 2020, following Tumblr shutting down the above account, Tumblr reported eight images and three videos containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "malco2334" with an email address of datece1785@ummoh.com. I downloaded and reviewed these images and videos, of which at least two images and two videos met the federal definition of child pornography. For example:

> File Name: 635546263383916544_0_inline_image.gifv
> MD5: 2149713c4ac18f18b7b1b1c0f9ce98ff
> The video depicted a female child laying on her back naked with her head close to a naked adult male. The female child was approximately 4 – 8 years of age. The adult male was masturbating above the child's face while brushing his hand against the chin of the female child.

/ / /

CyberTipline Report 83511841

40. Between December 6-8, 2020, following Tumblr shutting down the above account, Tumblr reported five images containing suspected child pornography were uploaded by the account created at **Target IP Address**, identified as "fuckyoungsluts" with an email address of dedokit733@menece.com. I downloaded and reviewed these images, of which at least four images met the federal definition of child pornography. For example:

> File Name: 636822037304836096_0_inline_image.jpg
> MD5: 00ba061500a9adf55bd4b87b5054c9f2
> The image depicts a female child and male child who were both naked. The female child was approximately 4 – 8 years of age; the male child was approximately 6 – 10. The female child had her hand wrapped around the erect penis of the male child.

41. During the review of the above CyberTipline Reports, I identified all the below accounts were created by the same IP address of 24.20.61.61 (**Target IP Address**) and that the first Tumblr-identified CEM post from each account would be from **Target IP Address**. Part of the records provided by Tumblr in their CyberTipline Reports included the IP addresses used to conduct each posting. Additionally, I learned that over 1/3rd of the nearly 1300 posts reported by Tumblr in the CyberTipline Reports were from the **Target IP address**; **BATES** used his internet to post approximately one third of all Tumblr-identified CEM across 14 accounts. Over 4% of the posts were associated with Verizon Wireless-owned IP addresses; Verizon is also the service provider for **BATES' Cell Phone**. All 14 accounts reported by Tumblr connected from the **Target IP Address** when Tumblr identified the first CEM-related post; this is consistent with all 14 accounts being controlled by one user. Additionally, I identified what appeared to be a pattern in which one Tumblr account was cancelled and another account was created shortly after, consistent with the user being the same between the 14 accounts. For example:

Cyber Tipline Report	Tumblr Account	Reported Email Address	Offending Post Date Range	Offending Post Time Range
80287864	jesusdidntsavemeforthis	jaredtbates1995@gmail.com (**Subject Email Account**)	9/22/20	5:28 p.m. – 6:43 p.m.
81100977	swimmingjudgeturtleroad	jaredtbates1995@gmail.com (**Subject Email Account**)	10/8/20	6:15 p.m. – 7:20 p.m.
81262604	innerfestivalsportsshepherd	jaredtbates1995@gmail.com (**Subject Email Account**)	10/10-10/11/20	10:56 p.m. – 10:05 p.m.
81602360	automaticmoneyfriendapricot	jonnyboyles@yahoo.com	10/17-10/18/20	9:22 p.m. – 9:18 p.m.
81606419	qualitywombateggthing	jonnyboyles@yahoo.com	10/18-10/19/20	8:34 p.m. – 3:08 a.m.
81948441	unlikelydeanroadeggs	malcommarkstrom@yahoo.com	10/24/20	5:28 p.m. – 6:40 p.m.
81961358	sparklymoneyathletepanda	malcommarkstrom@yahoo.com	10/24/20	11:43 p.m. – 11:48 p.m.
82499408	fantasticathletemuffinpasta	malcommarkstrom@yahoo.com	10/31/20	8:43 p.m. – 10:17 p.m.
82675833	partyboy20	totov96409@diide.com	11/6-11/8/20	8:00 p.m. – 8:36 p.m.
82675741	humongousfestivalskeletonzonk	gexiv65905@jqjlb.com	11/8-11/9/20	9:25 a.m. – 5:00 a.m.
84314253	humongousfestivalskeletonzonk	gexiv65905@jqjlb.com	11/8-11/9/20	9:25 a.m. – 5:00 a.m.
82780966	malcyboysbackformore	nadoy43272@testbnk.com	11/12-11/13/20	6:34 p.m. – 3:39 a.m.
82874529	illalwayscomeback	wixose2120@testbnk.com	11/13-11/15/20	5:30 p.m. – 8:38 p.m.
83072099	malco2334	datece1785@ummoh.com	11/22-11/23/20	8:01 p.m. – 6:28 a.m.
83511841	fuckyoungsluts	dedokit733@menece.com	12/06-12/8/20	10:00 p.m. – 3:45 p.m.

/ / /

/ / /

/ / /

Investigators Subpoena Utility Records and Identify BATES

42. Before the investigation was assigned to SA Lindsly, the Oregon ICAC Task Force served a subpoena on Comcast for records related to 24.20.61.61 (**Target IP Address**). Comcast's records revealed that the subscriber for the **Target IP Address** was:

> Name: Jared T. Bates
> Address: 562 SW 257TH Avenue Apartment 35, Troutdale, Oregon 97060-7407 (BATES' Former Residence)
> Activation Date: Unknown

43. Based on the above information and utilizing law enforcement databases, SA Lindsly was able to identify **Jared Tyler BATES** as having date of birth XX/XX/1995 and Oregon Driver License #XXXX867. At this period of time, **BATES'** DMV reported address of record was a PO Box. However, as described below, **BATES's** current DMV reported address is the **Subject Premises**. SA Lindsly, through open-source research, also identified a potential co-occupant and/or girlfriend of **BATES** as Amanda Tolva. According to DMV records, Amanda Tolva had a reported address of BATES's Former Residence. I believe that Amanda Tolva might be the girlfriend of BATES' based on similar ages and different last names. No other occupants of BATES's Former Residence were identified.

44. In March 2021, SA Lindsly attempted to contact the property manager responsible for **BATES**' Former Residence in order to serve a subpoena for records. During the telephone call with the manager, the manager stated that **BATES** would be moving out shortly. Additionally, the property management never complied with the subpoena nor provided SA Lindsly with rental records.

45. On March 30, 2021, SA Lindsly served an administrative subpoena on Portland General Electric (PGE), a utility provider for the Portland-metro area, for records related to **BATES**, Amanda Tolva, and 562 SW 257th Avenue #35, Troutdale, Oregon 97060 (BATES'

Former Residence). PGE provided responsive records on April 7, 2021, which confirmed that Amanda Tolva was the previous subscriber at that address (**BATES**' Former Residence) and that **BATES** was not a customer registered with PGE. **BATES**' phone number, 971-806-2573 which is reported on the application for the **Subject Premises**, appeared in the PGE records as an additional phone for Amanda Tolva. According to open-source queries (www.freecarrierlookup.com), I learned that phone number 971-806-2573 (**BATES' Cell Phone**) is serviced by Verizon Wireless, consistent with IP connectivity logs reported by Tumblr.

46. On June 22, 2021, SA Lindsly served another administrative subpoena on PGE for utility records in the name of **BATES** and Amanda Tolva in an attempt to locate their current residence. According to records provided by PGE, I learned that Amanda Tolva was the subscriber at 21961 NE Chinook Way #229, Fairview, Oregon 97024 (**Subject Premises**) and has been since March 22, 2021, consistent with the property manager stating that **BATES** was moving out of **BATES'** Former Residence. **BATES**' phone number, 971-806-2573 which is reported on the application for the **Subject Premises**, appeared in these PGE records as well, showing as an additional phone for Amanda Tolva.

47. According to current DMV records, I learned that **BATES** has a reported address of the **Subject Premises**.

48. On June 22, 2021, SA Lindsly served an administrative subpoena on Chinook Way Apartments, the property management group for the **Subject Premises**, for records related to **BATES**, Amanda Tolva, and 21961 NE Chinook Way #229, Fairview, Oregon 97024 (**Subject Premises**). Chinook Way provided responsive records on June 25, 2021.

/ / /

49. According to those records, I learned that **BATES** and Amanda Tolva reside at 21961 NE Chinook Way #229, Fairview, Oregon 97024 (**Subject Premises**) and have been since March 22, 2021. Additionally, I learned that **BATES** and Amanda Tolva used an iPhone from the IP address 24.20.61.61 (**Target IP Address**) in order to sign the rental application and agreement. As discussed above, this was the same IP address that was identified in all 17 CyberTipline Reports distributing child pornography. Furthermore, according to the rental records **BATES** listed his former residence as 562 SW 257th Avenue Apartment 35, Troutdale, Oregon 97060 (**BATES'** Former Residence). **BATES** and Amanda Tolva both listed jaredtbates1995@gmail.com (**Subject Email Address**) as their email contact on the application, which was the associated email address in three of the CyberTipline Reports related to the distribution of child pornography. Based on the fact that the same IP address (**Target IP Address**) that accessed the Tumblr accounts identified to distribute child pornography was also used by **BATES** and Amanda Tolva to execute a new lease agreement at the **Subject Premises** and the fact that **BATES** and Amanda Tolva reported on their lease at the **Subject Premises** that their email address (**Subject Email Address**) was the same email account linked to several of the Tumblr accounts identified to distribute child pornography, I believe that **BATES** controlled the various Tumblr accounts.

50. On July 23, 2021, I served an administrative subpoena on Google LLC, the operator of the Gmail and provider for **Subject Email Address** which **BATES** included in his apartment application. During my review of the records, I learned that the **Subject Email Address** was accessed approximately 168 times between January 1 – August 13, 2021. The **Subject Email Address** was accessed by various IP addresses, most of which appeared to be serviced by Comcast Cable Communications.

51. On July 28, 2021, I served an administrative subpoena on Comcast to obtain subscriber records on several of the IP addresses used to access the **Subject Email Account**. I requested subscriber records on various IP addresses that accessed the **Subject Email Account** on April 1 – July 16, 2021, consistent with **BATES'** recent move into the **Subject Premises**. During a review of the provided records by Comcast, I learned that in each instance the internet that was used to access the **Subject Email Account** was subscribed to **BATES** at the **Subject Premises**. Furthermore, the internet account is still active at the **Subject Premises**.

52. Based on the above information, I believe that **BATES** resides at the **Subject Premises**, that **BATES** owned and controlled the Tumblr accounts that were distributing child pornography with an email in his namesake (**Subject Email Account**), that **BATES** accessed these accounts using the internet service at **BATES'** former residence, and that **BATES'** continues to access the **Subject Email Account** from internet subscribed in his name to the **Subject Premises**. Additionally, **BATES** used the **Target IP Address** to execute his new lease agreement at the **Subject Premises**.

53. Upon moving to Chinook Way Apartments (**Subject Premises**) **BATES**' Comcast-provided internet service was no longer utilizing a static IP address; a static IP address is issued by the internet service provider and is continually assigned to a household or device. **BATES**' current internet service uses a dynamic IP address, which is essentially a rotating, on-demand IP address, provided by Comcast for a short duration; dynamic addresses mean more people can use a limited number of IP addresses within a range or block of IP addresses reserved by an Internet Service Provider. Comcast retains records regarding the internet user of each dynamic IP address; when a user's temporary IP address is assigned to a different user, Comcast records that information. As reported by Google, **BATES** accessed **Subject Email Account**

from multiple IP addresses; when queried, Comcast confirmed that BATES paid for the internet service which is associated with many of these connections to Gmail. Other connections to **Subject Email Account** appear to be from a device using Verizon Wireless or a VPN, which is consistent with activity reported by Tumblr in most of the CybertTipline Reports. Investigators have been unable to identify new CyberTipline Reports from an IP address originating from the **Subject Premises**, likely due to Comcast assigning a dynamic IP address to **BATES'** current internet service (i.e. it changes frequently)**.** Despite this**,** I believe that evidence of the **Target Offenses** will still be located at the **Subject Premises** and/or on the person of BATES.

54. I know that social media applications, including Tumblr, are frequently accessed by cellular devices and/or tablets (mobile communications devices). Based on my training and experience involving mobile communication devices, I know these devices are commonly transported by the user on their person, in the user's vehicle, and are connected to the user's computer or computers via a USB connection cable. Users typically maintain software to communicate with the mobile communication devices in the residence or work on computers and then transfer or synchronize the data on the device with the data on the computers. The purpose of this procedure is so the user has all data on the device and their computers at the user's disposal. This data can include personal or business contacts, calendar entries, notes or memos, and videos & images. Users typically transport the mobile communications device between their residence and workplace daily. As this device serves as a mobile telephone, users typically carry the device on their person and maintain it nearby when at work or home. As such, I believe that evidence of the **Target Offenses** will likely be found on the person of **BATES** (including any cell phone on his person including **BATES's Cell Phone**), the **Subject Premises**, and the **Subject Email Account**.

55. The **Subject Premises** is a multi-family apartment located at 21961 NE Chinook Way #229, Fairview, Oregon 97024. The **Subject Premises** is a grey three-story building with white colored trim; there is a stone marker on the south side labeled "Douglas 21061". The front door is an interior door. Photos of the **Subject Premises** appear in Attachment A-1.

Search and Seizure of Digital Data

56. This application seeks permission to search for and seize evidence of the crimes described above, including evidence of how computers, digital devices, and digital storage media were used, the purpose of their use, and who used them.

57. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that data in digital form can be stored on a variety of systems and storage devices, including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media in phones and cameras, personal music devices, and similar items.

Removal of Data Storage Devices

58. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during a search of premises it is not always possible to create a forensic image of or search digital devices or media for data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of

digital devices and software in use today, it is difficult to anticipate all of the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data not readily apparent to the casual user. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it is generally impractical to search for data during the execution of a physical search of premises. Storage devices capable of storing 500 gigabytes to several terabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

Laboratory Setting May Be Essential for Complete and Accurate Analysis of Data

59. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

/ / /

60. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue that may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

61. *Latent Data*: Searching digital devices can require the use of precise scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, they can be recovered months or years later using readily available

forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

62. *Contextual Data*:

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard

drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software, may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

63. In searching for data capable of being read, stored, or interpreted by a computer or storage device, law enforcement personnel executing the search warrants will employ the following procedure:

a. *On site search, if practicable*. Law enforcement officers trained in computer forensics (hereafter, "computer personnel"), if present, may be able to determine if digital devices can be searched on site in a reasonable amount of time and without jeopardizing the ability to preserve data on the devices. Any device searched on site will be seized only if it contains data falling within the list of items to be seized as set forth in the warrants and in Attachment B.

b. *On site imaging, if practicable*. If a digital device cannot be searched on site as described above, the computer personnel, if present, will determine whether the device can be imaged on site in a reasonable amount of time without jeopardizing the ability to preserve the data.

c. *Seizure of digital devices for off-site imaging and search*. If no computer personnel are present at the execution of the search warrant, or if they determine that a digital device cannot be searched or imaged on site in a reasonable amount of time and without jeopardizing the ability to preserve data, the digital device will be seized and transported to an appropriate law enforcement laboratory for review.

d. Law enforcement personnel will examine the digital device to extract and seize any data that falls within the list of items to be seized as set forth in the warrant and in Attachment B. To the extent they discover data that falls outside the scope of the warrant that they believe should be seized (e.g., contraband or evidence of other crimes), they will seek an additional warrant.

e. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a "hash value" library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data falls within the list of items to be seized under the warrant.

f. If the digital device was seized or imaged, law enforcement personnel will perform an initial search of the original digital device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to the warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether an original digital device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete the search of the digital device or image within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

g. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on an original digital device or image do not contain any data that fall within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement

personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

h. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that original data device and will seal any image of the device, absent further authorization from the Court.

Items to be Seized

64. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

/ / /

c. Any magnetic, electronic, or optical storage device capable of storing data, such as thumb drives and other USB data storage devices, floppy disks, hard disks, tapes, CD ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, iPods, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store the types of contraband and evidence, fruits, or instrumentalities of such crimes, as set forth in Attachment B;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to upload, download, store, receive, possess, or view child pornography, including the web browser's history; temporary Internet files; cookies, bookmarked or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, internet relay chat, instant messages, and other electronic

communications; address books; contact lists; records of social networking and online service usage; usernames or screen names; and software that would allow others to control the digital device such as viruses, Trojan horses, and other forms of malicious software.

Retention of Image

65. The government will retain a forensic image of each electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

66. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrants return to the Court will describe the physical storage media that were seized or imaged.

67. The government has made no prior effort in any judicial forum to obtain the materials sought in these requested warrants.

Conclusion

68. Based on the foregoing, I have probable cause to believe that **Jared BATES** committed the **Target Offenses** and that contraband and evidence, fruits, and instrumentalities of those violations will be located on his person, contained in **BATES' Cell Phone**, the **Subject Email Account**, and at the **Subject Premises** as described above and in Attachment A-1 & A-2. I therefore respectfully request that the Court issue warrants authorizing searches of **Jared BATES'** person, **BATES' Cell Phone** or any device found on the person of **BATES'**, the

Subject Email Account, and the **Subject Premises** as described in Attachment A-1 & A-2, for the items listed in Attachment B-1 & B-2, and authorizing the examination and seizure of any such items found.

69. Prior to being submitted to the Court, this affidavit, the accompanying applications, and the requested search warrants were all reviewed by Assistant United States Attorney (AUSA) Scott Kerin. AUSA Kerin advised me that in his opinion, the affidavit and applications are legally and factually sufficient to establish probable cause to support the issuance of the requested warrants.

Request for Precluding Notice

70. It is respectfully requested, pursuant to 18 U.S.C. § 2705(b), that Provider be ordered not to disclose the existence or service of the search and seizure warrant to the subscriber, customer, or any other person, for a period of one year from the date of said order (unless that period is extended by further order of the Court), except as required to disclose to Provider's officers, employees, or agents to the extent necessary to comply with the warrant. Based upon my knowledge, training, and experience, it is my belief that notification at this time of the existence of the warrant will result in the endangerment of the life or physical safety of an individual, flight from prosecution, the destruction of or tampering with evidence, intimidation of potential witnesses, and/or otherwise seriously jeopardize an investigation.

Request for Sealing

71. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search warrant, including the application, this affidavit, the attachments, and the requested search warrant. I believe that sealing these documents is necessary because the information to be seized is relevant to an

ongoing investigation, and any disclosure of the information at this time may (include all of the following that apply: endanger the life or physical safety of an individual, cause flight from prosecution, cause destruction of or tampering with evidence, cause intimidation of potential witnesses, or otherwise seriously jeopardize an investigation). Premature disclosure of the contents of the application, this affidavit, the attachments, and the requested search warrant may adversely affect the integrity of the investigation.

By telephone
JUSTIN MOSHOFSKY
HSI Special Agent

Sworn to telephonically pursuant to Fed. R. Crim. P. 4.1 at 12:03 p.m. on September 3, 2021.

Stacie F. Beckerman
HONORABLE STACIE F. BECKERMAN
United States Magistrate Judge